Kapitel 2:

Gefahren im Netz: Geschichten aus dem Leben

Immer wieder ist zu lesen, dass es Hacker und Betrüger auf Ihre Daten und Ihr Geld abgesehen haben. Oft genug wird hier mit Fachbegriffen hantiert und ist die Warnung recht abstrakt, d.h. für den Normalbürger nicht greif- und damit schwer verstehbar. Lassen Sie uns daher mit Geschichten aus dem realen Leben beginnen. So können Sie die Gefahrensituation miterleben und somit die Vorgehensweise der Betrüger verstehen und Gegenmaßnahmen ergreifen.

Schadsoftware: Die Nachricht ist nicht allein (Malware)

Eines der schon klassischen Einfallstore für Schadprogramme (Viren, Würmer, Trojaner etc.) und Schadsoftware (Malware) ist eine Nachricht, in deren Anhang sich eine schadenverursachende Datei befindet oder die einen Link enthält, über den ein schadenverursachendes Programm heruntergeladen werden könnte.

Schadprogramme sind voll funktionsfähige und oft eigenständige Programme mit versteckten Funktionen, um auf dem betroffenen Computer Daten z.B. zu löschen, zu zerstören oder zu verändern. Mit dem ersten Anklicken kommt es zur Ausführung des Programms.

Wenn wir hier von Nachricht sprechen, dann ist dies ein erster Hinweis für Sie, dass es sich nicht nur um E-Mails handelt, sondern auch andere Nachrichten z.B. über Messenger-Dienste (Facebook, Instagram etc.) infiziert sein können.

Mails mit schadenverursachenden Anhängen

BEISPIEL

Manfred Zangerl erhält beruflich viele E-Mails, und oft auch E-Mails von Freunden und Geschäftspartnern, an denen eine Datei angehängt ist, oft reine PDF-Dateien, immer wieder aber auch Word- oder Excel-Dokumente. Bei vertrauenswürdigen Absendern öffnet oder speichert Manfred Zangerl die Dateien direkt. Jetzt aber ließ er seinen Computer einmal professionell kontrollieren. Und stellte überrascht und auch konsterniert fest, dass auf dem Computer mehrere Schadprogramme vorhanden waren.

Was war geschehen? Manfred Zangerl war zwar vorsichtig und öffnete nur Dateien, die ihm von vertrauenswürdigen Personen geschickt wurden. Allerdings können auch diese unwissentlich mit infizierten Dateien gearbeitet und diese dann weitergegeben haben. Das Ausmaß der potenziellen Gefährdung wird deutlicher, wenn man sich einmal ansieht, wie unterschiedlich Viren und Schadsoftware arbeiten.

- **Dateiviren:** Im Allgemeinen sind hier Schadprogramme gemeint, die sich in Computerprogramme kopieren und dann bei jedem Aufruf weiterverbreitet werden.
- **Makroviren** kommen in Word- und Excel-Dateien vor. Ein Makro ist eine Folge von Befehlen, die automatisch aufgerufen werden und so zu Arbeitserleichterungen führen. In dieser Befehlskette können sich kleine Schadprogramme einnisten und verstecken. Die Schadensroutinen gehen hierbei von einfachen Scherzen bis hin zum Löschen von Dateien.
- **Computerwurm** (kurz **Wurm**) ist ein Schadprogramm mit der Eigenschaft, sich selbst zu vervielfältigen, nachdem es einmal ausgeführt worden ist. In Abgrenzung zum Computervirus verbreitet sich der Wurm über Netzwerke oder über Wechselmedien wie USB-Sticks selbstständig.
- **Trojanische Pferde** sind kleine Schadprogramme, die sich in anderen Programmen einnisten. Je nach Ausgestaltung laden diese selbstständig andere Schadprogramme auf den Computer oder spähen Daten des Nutzers wie Kontozugangsdaten aus und versenden diese an den Betrüger.
- **Residente Viren** nisten sich im Arbeitsspeicher ein und infizieren von dort aus Datenträger wie USB-Sticks.
- **Tarnkappenviren (Stealth-Viren)** sind in der Lage, die Aktivität von Antivirensoftware zu erkennen und sich während dieser Aktivität zu verstecken.
- **Polymorphe Viren** verändern laufend ihre Gestalt, d.h. ihren Code. Hierdurch sind sie für Antivirensoftware schwer erkennbar.
- **Script-Viren** können sich in HTML-Codes (HTML: Hypertext Markup Language, Texte mit Hyperlinks, …) verstecken. Sie kommen in E-Mails vor, die das HTML- statt das Textformat verwenden.

Und auch in Videos können kleine Schadprogramme enthalten sein, wie die Angriffe 2017 auf das deutsche Verteidigungsministerium und 2020 auf das österreichische Außenministerium zeigen. Hier gab es jeweils mehrere E-Mails mit einem internen Absender (siehe „Die persönliche[re] Mail“ in Kapitel 2) mit Weihnachtsgrüßen und einem Video zum Fest. Dieses wurde von mehreren Empfängern geöffnet und ermöglichte den Angreifern so Zugriff auf die Rechner und das Netzwerk.

Bei den Schutzmaßnahmen muss man sich auch vor Augen halten, dass etwa eine Milliarde Viren und andere Schadprogramme bekannt sind und täglich mehrere hunderttausend neu entdeckt werden.

Antivirenprogramme reagieren auf bekannte Viren. Beim Durchsuchen von Daten werden verdächtige Codes mit einer umfangreichen Datenbank bekannter Schadprogramme abgeglichen. Gibt es einen Treffer, schlägt das Programm Alarm und blockiert die weitere Ausführung des Schadprogramms. Das bedeutet, ein Antivirenprogramm ist nur gut, wenn die dahinterliegende Datenbank auf dem neuesten Stand ist. Daher müssen die Hersteller von Antivirenprogrammen ihre Datenbanken täglich mit den neuen Schadsignaturen ergänzen und die Antivirenprogramme aktualisieren. Trotzdem besteht immer die Gefahr, dass ganz neue Schädlinge nicht erkannt werden.

TIPP

Wie können Sie sich schützen? Wir greifen hier auf Empfehlungen der deutschen Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) (siehe Adressen/Links) zurück:

- ➜ Nutzen Sie Virenschutz-Software und führen Sie automatische Updates durch.
- ➜ Laden Sie/kaufen Sie Virenscanner nur bei vertrauenswürdigen Anbietern.
- ➜ Löschen Sie verdächtige E-Mails, das ist immer ohne Gefahr möglich. Verdächtig sind E-Mails, wenn sie Folgendes aufweisen:
  - Unbekannter Absender mit Sonderzeichen in der Adresse
  - Unbekannter Absender ohne Betreff
  - Unbekannter Absender, verwendet Englisch oder eine andere Fremdsprache
  - Unbekannter Absender, der die Mail an „Recipients“ etc., d.h. nicht an Sie persönlich versendet hat
- ➜ Stellen Sie die Sicherheitseinstellungen Ihres E-Mail-Programms so ein, dass ein Script nicht automatisch ausgeführt wird.
- ➜ Öffnen Sie niemals eine ZIP-Datei, die Sie von einem unbekannten Absender erhalten haben. Bei ZIP-Dateien von einem bekannten Absender fragen Sie ggfs. nach, was der Inhalt ist.

- ➜ Öffnen Sie keine ausführbare Datei, die Sie an Endungen wie „.exe“, „.bat“, „.com“ oder „.vbs“ erkennen, ungeprüft. Fragen Sie im Zweifelsfall beim Absender nach.
- ➜ Seien Sie vorsichtig im Umgang mit HTML-E-Mails.
- ➜ Versenden Sie selbst auch keine Anhänge, die Sie aus unsicheren Quellen haben.

Mails mit Links zu schädlichen Webseiten

BEISPIEL

Katharina Li bekam einen Anruf von einem guten Freund: „Du, dein E-Mail-Account wurde gehackt. Bitte warne alle deine Kontakte.“ Im Nachgang schickte ihr Freund auch das fragliche E-Mail:

Was war geschehen? Katharina hatte ihrerseits von einem Freund eine E-Mail ähnlichen Inhalts und Aussehens erhalten – und aufgrund des bekannten Namens auch den Link angeklickt und sich hierdurch infiziert, Schadsoftware auf ihren Computer geladen. Und diese Schadsoftware verschickt seitdem an die Adressen in ihrem Mail-Adressbuch diese Mails.

Eine andere Masche von Betrügern ist es, ihre Mail einem aktuellen Thema zu widmen, z.B.: „So schützen Sie sich gegen das Coronavirus“, „Die ersten

Unfallbilder von Michael Schumacher“. Diese sollen einen seriöseren Eindruck vermitteln, den Leser neugierig machen und dazu verleiten, die Mail und anschließend auch den Link zu öffnen.

TIPP

Schützen können Sie sich gegen diese Art von Mails durch ein gesundes Misstrauen. Wir gehen hierbei kurz auf einige Punkte der konkreten Mail ein, die Sie stutzig machen sollten:

Absender

Den Absender in Klarschrift (hier: „K8brei“) kennen Sie und vertrauen ihm. Dieser erscheint auch in der Mailliste. Gehen Sie jedoch in die Mail, so sehen Sie auch den Absender, der oft nicht gefälscht wird. In diesem Fall ist dies mohammed@bemah.net, der mit dem scheinbaren Absender wahrscheinlich nichts gemein hat.

Betreffzeile

Zumeist ist diese leer. Entspricht es der Gewohnheit Ihres Bekannten, Ihnen eine Mail ohne Betreff zu schicken? Oder ist der Betreff sehr reißerisch und soll Sie neugierig machen?

Inhalt der Mail

In der Mail befindet sich nur ein Link zu einer Webseite. Keine Anrede, kein Text, kein freundliches Wort vom Absender, keine Unterschrift. Entspricht es der Gewohnheit Ihres Vertrauten, Ihnen eine Mail ohne jede Freundlichkeitsformel zu senden?

Bei auch nur geringstem Misstrauen sollten Sie den Link in dieser Mail nicht anklicken! Greifen Sie lieber zum Telefon und fragen Sie nach, was es mit der Mail auf sich hat.

Möchten Sie Ihr Wissen über und Ihre Widerstandskraft gegen Spam-Mails testen? Dann können Sie dies mit einem kostenlosen Test bei der SoSafe GmbH in Köln über das Internet machen: https://phish-test.de/. Sie erhalten dann drei so genannte Phishing-Mails, jedoch ohne gefährlichen Inhalt. Verhalten Sie sich bei diesen Mails falsch, indem Sie z.B. den Link öffnen, so kommen Sie auf eine Lernseite, auf der Ihnen Ihr Fehler erklärt wird.

Und so sieht hoffentlich auch Ihr Ergebnis nach dem Test aus:

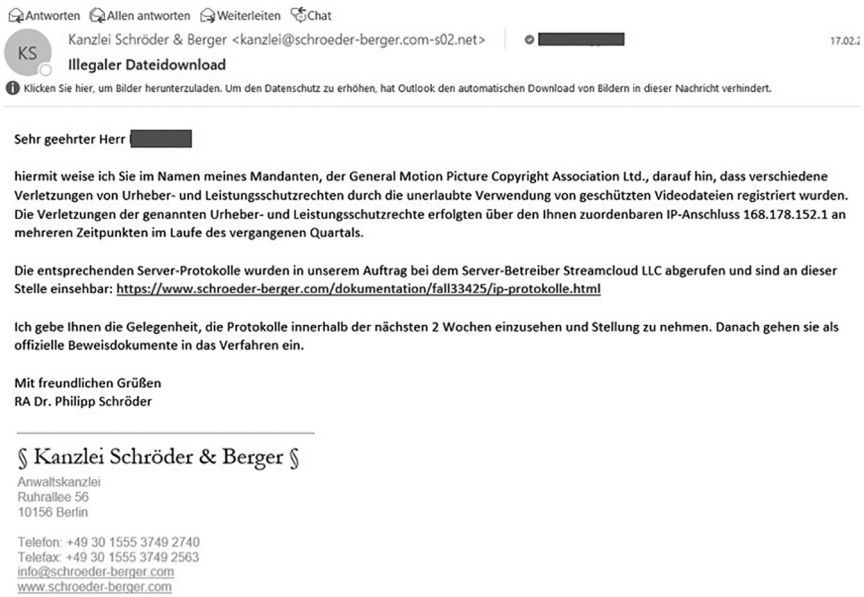
Haben Sie die Mails alle erkannt? Oder sind Sie uns auch einmal "ins Netz gegangen"? So haben Sie abgeschnitten:

Versendete E-Mails:	Schwierigkeitslevel:	Ergebnis:
Anwalt illegaler Download	Leicht	Nicht geklickt
Neues TAN Verfahren	Mittel	Nicht geklickt
Schenkung	Schwer	Nicht geklickt

Haben Sie vielen Dank für Ihre Teilnahme an dieser Aktion.

Sie wollen auch Ihre Freunde, Familie oder Kollegen auf unsere Aktion aufmerksam machen? Dann teilen Sie den Link zu www.phish-test.de doch sehr gerne in den von Ihnen genutzten sozialen Netzwerken - und helfen Sie uns dabei, alle zum Thema Phishing aufzuklären!

Da es sich bei Mails mit einem schädlichen Link um ein für Betrüger besonders interessantes Thema zu handeln scheint, bringen wir ein weiteres Beispiel:



Antworten Allen antworten Weiterleiten Chat

KS Kanzlei Schröder & Berger <kanzlei@schroeder-berger.com-s02.net> [redacted] 17.02.

Illegaler Dateidownload

Klicken Sie hier, um Bilder herunterzuladen. Um den Datenschutz zu erhöhen, hat Outlook den automatischen Download von Bildern in dieser Nachricht verhindert.

Sehr geehrter Herr [redacted]

hiermit weise ich Sie im Namen meines Mandanten, der General Motion Picture Copyright Association Ltd., darauf hin, dass verschiedene Verletzungen von Urheber- und Leistungsschutzrechten durch die unerlaubte Verwendung von geschützten Videodateien registriert wurden. Die Verletzungen der genannten Urheber- und Leistungsschutzrechte erfolgten über den Ihnen zuordenbaren IP-Anschluss 168.178.152.1 an mehreren Zeitpunkten im Laufe des vergangenen Quartals.

Die entsprechenden Server-Protokolle wurden in unserem Auftrag bei dem Server-Betreiber Streamcloud LLC abgerufen und sind an dieser Stelle einsehbar: https://www.schroeder-berger.com/dokumentation/fall33425/ip-protokolle.html

Ich gebe Ihnen die Gelegenheit, die Protokolle innerhalb der nächsten 2 Wochen einzusehen und Stellung zu nehmen. Danach gehen sie als offizielle Beweisdokumente in das Verfahren ein.

Mit freundlichen Grüßen
RA Dr. Philipp Schröder

§ Kanzlei Schröder & Berger §
Anwaltskanzlei
Ruhrallee 56
10156 Berlin

Telefon: +49 30 1555 3749 2740
Telefax: +49 30 1555 3749 2563
info@schroeder-berger.com
www.schroeder-berger.com

Sie werden also von einem Anwalt aus Berlin angeschrieben, der Ihnen illegalen Video-Download vorwirft. Nun, wer hat sich in youtube.com nicht schon einmal Videos angesehen? Aber diese sollen illegal sein? Noch unter Schock stehend wollen Sie sich die Beweise des Anwalts ansehen.

TIPP

Nun, das sollten Sie nicht so schnell tun! Denn es könnte sich auch um eine geschickte Falle handeln:

- ➜ Anwälte versenden ihre Mahnschreiben per Post und nicht per E-Mail!
- ➜ Die Rechtsanwaltskanzlei muss nicht echt sein:
  - Geben Sie die Homepage der Kanzlei in Ihren Browser ein (nicht kopieren). In diesem Fall wird die Homepage nicht gefunden.
  - Geben Sie den Namen der Kanzlei bei der zuständigen Rechtsanwaltskammer ein, in diesem Fall bei der Rechtsanwaltskammer Berlin (www.rak-berlin.de). Auch hier wird die Kanzlei nicht gefunden!
- ➜ Fahren Sie mit dem Cursor leicht (nicht anklicken!) über den angegebenen Link. Sie sehen hier eine andere Adresse, die mit der Klarschrift nichts zu tun hat.

Ergebnis: Dies ist eine Fälschung (Fake-Mail) mit einem Link, der Sie mit hoher Wahrscheinlichkeit zu einer schädlichen Seite führt. Finger weg!

Die zweitgrößte Gefahr neben den Mails mit versautem Anhang, sich ein Schadprogramm einzufangen, besteht beim Surfen im Netz. Allein durch den Besuch einer manipulierten Webseite kann Ihr Computer mit einem Schadprogramm infiziert werden (Fachbegriff: „Drive-By-Infektion"). Dabei kann es sich durchaus auch um seriöse und vielbesuchte Seiten handeln, die unbemerkt für betrügerische Zwecke missbraucht werden.

Wie kann das passieren? Der Computernutzer ruft eine Internetseite auf. Für Betroffene ist nicht erkennbar, dass die Seite manipuliert ist. Heimlich wird ein Programm auf den Opfer-Computer geladen, das den Rechner auf Schwachstellen untersucht. Die gesammelten Daten werden genutzt, um

Schadprogramme an den Opfer-Computer zu schicken, wenn es sich für den Angreifer „lohnt".

Eine Drive-By-Infektion kann man sich mit jedem Internetbrowser einfangen. Je aktueller aber die Version des Browsers ist, desto geringer ist die Gefahr, dass sich eine Drive-By-Infektion auf dem Computer einschleicht. (Vgl. www.drive-by-download.de)

Twitter Spams

BEISPIEL

Michaela Cerna ist zwar eher eine Freundin der vielen Worte, nicht jedoch bei der textlichen Kommunikation. Hier ist sie eine bekennende Anhängerin des Kurznachrichtendiensts Twitter, der jede Botschaft auf 280 Zeichen begrenzt. Das reicht natürlich nicht immer aus, um Freundinnen auf eine besondere Webseite aufmerksam zu machen. Aber zum Glück kann man in Twitter auch mit der platzsparenden URL (Uniform Ressource Locator: identifiziert den Ort einer Webseite im Internet) arbeiten. Michaela erhält diese auch von ihren Freundinnen und nutzt sie natürlich auch selbst. Auch gestern. Und seither arbeitet ihr Smartphone sehr langsam. Möglicherweise hat sie sich einen Krypto-Miner (Krypto-Mining-Schadprogramme missbrauchen Ihren PC oder Ihr Smartphone zum Erzeugen von digitalem Geld) eingefangen?

Was war geschehen? Betrüger nutzen die kurze URL dazu, die richtige Adresse zu verschleiern. Klickt jemand auf die URL, so gelangt er zu der Seite der Betrüger und kann sich hier mit einem Krypto-Miner oder auch Schlimmerem infizieren. Die Twitter-Nachricht kam aber von einer Freundin. Wie kommen denn jetzt hier Betrüger ins Spiel? Die Anti-Spam-Experten des Sicherheitsunternehmens BitDefender (pcmagazin 2009) haben bereits im Jahr 2009 einige der Tricks aufgedeckt und mit sprechenden Namen kategorisiert:

- **ReTweet-Spam:** Diese Art Spam sucht nach legitimen, ungefährlichen Tweets innerhalb von Twitter und re-postet diese mit dem Zusatz einer gefährlichen URL.

- **Trend-Spam:** Hier suchen Cyberkriminelle nach aktuellen Themen (Hot Topics) – beispielsweise geschehen nach dem Tod von Michael Jackson – und schalten eigene Tweets zum Thema mit dem Verweis auf infizierte Websites.
- **Tweet Spam**: Diese Art Spam wird über die sogenannten Follower (zu Deutsch: „Anhänger"; Follower sind Internetnutzer auf sozialen Netzwerken, die anderen Internetnutzern folgen) verbreitet. Indem diese den Tweet eines Spam-Opfers lesen, verbreitet sich die Nachricht weiter.

Auch die Freundin kann also einem Betrüger aufgesessen sein oder von diesem benutzt werden und so die falsche URL weiterverbreiten. Nur auf den bekannten Absender zu vertrauen, reicht also nicht aus.

Wie können Sie sich hiervor schützen?

TIPP

Seien Sie sehr zurückhaltend beim Anklicken einer URL, die in Twitter immer nur 23 Zeichen umfasst. Und sollten Sie einem Link folgen, so prüfen Sie die Seite auf Vertrauenswürdigkeit. Hierfür würde z.B. das „https" statt „http" in der Adresszeile sprechen. Vertrauliche Daten wie den Namen des Users und das Passwort sollten Sie in keinem Fall eingeben, rufen Sie hierfür die Webseite Ihrer Bank, des Internethändlers etc. auf dem üblichen Weg auf.

Krypto-Miner auf dem PC

BEISPIEL

Lisa Franken hat einen etwas älteren Computer, bereits außerhalb der Gewährleistung, und stellt erstaunt fest, dass irgendetwas nicht ganz zu stimmen scheint. Immer wieder ist die Lüftung sehr laut, scheint der Computer schon fast „zu röcheln". Und alles geht sehr langsam. So benötigt es mehrere Sekunden, bis sich Dateien öffnen lassen, und der Seitenaufbau im Internet erfolgt sehr zögernd. Also ein Fall für eine Neuanschaffung?

Was war geschehen? Lisa Franken war einige Tage zuvor auf einer anderen als den üblicherweise von ihr besuchten Internetseiten. In diese Webseite war ein Javascript, also ein kleines Programm eingebunden, das bereits durch den Aufruf der Webseite auf den Computer des Besuchers übertragen wird. Ein bekannteres dieser Programme ist „Coinhave", welches ohne großen Aufwand von Webseitenbetreibern in ihre Seite eingebunden werden kann. Diese erhalten dann ein Entgelt für die Tätigkeit des Programms auf den Computern der Nutzer.

Und diese Tätigkeit ist das „Schürfen von Krypto-Währungen", weshalb hier auch von Krypto-Miner gesprochen wird. Diese Krypto-Währungen wie Bitcoin, Ethereum oder Monero entstehen durch kryptografische Berechnungen. Und diese kosten Rechnerzeit und Strom. Die Betreiber der Krypto-Miner wollen einerseits die Früchte des Schürfens erhalten, andererseits die Belastungen von Rechnerzeit und Stromkosten auf Sie verlagern.

Äußere und für Sie feststellbare Zeichen eines Krypto-Mining auf Ihrem Computer ist eine deutliche Verlangsamung der Abläufe und eine sehr aktive, d.h. laute Lüftung. Bei einer Analyse des Computers ist dann zumeist feststellbar, dass es einen oder mehrere Prozesse auf dem Computer gibt, die den Großteil der Rechenleistung (CPU) verwenden.

TIPP

Einen Basisschutz bieten laut Dombach (2018) die nachfolgenden Aktivitäten:

- Aktuelle Antimalware-Tools (Antivirensoftware) nutzen: Es gibt bekannte Miner, die sich so entdecken bzw. verhindern lassen.
- Im Browser Javascript deaktivieren bzw. nur zwingend erforderliche Scripts zulassen: sofern möglich, da Skriptsprachen oft essentielle Komponenten einer Webseite abbilden.
- Im Browser Anti-Krypto-Miner-Option aktivieren: sofern verfügbar bzw. unterstützt.
- Einsatz von Software, die Werbung blockiert: verhindert teilweise das Nachladen von Miner-Tools über die Webseite.